CLAIMS

What is claimed is:

1. A method for preventing information losses due to network node failure, the method comprising the steps of:

operatively connecting at least one backup node to a primary node;

synchronizing the at least one backup node and the primary node;

receiving, from a first endpoint, ingress traffic in the primary node;

replicating the ingress traffic to the at least one backup node;

outputting, from the primary mode, primary egress traffic;

outputting, from the at least one backup node, backup egress traffic;

determining if the primary node has failed;

transmitting, to a second endpoint, the primary egress traffic if it is determined that the primary node has not failed; and

transmitting, to the second endpoint, the backup egress traffic from a selected one of the at least one

backup nodes if it is determined that the primary node has failed,

wherein the backup egress traffic from the selected one of the at least one backup nodes replaces the primary egress traffic to the second endpoint and the backup node becomes the primary node for subsequent traffic.

2. The method of claim 1, wherein the primary node and the at least one backup node are network routers.

3. The method of claim 1, wherein the primary node and the at least one backup node are security engines for receiving encrypted ingress traffic and outputting decrypted egress traffic.

4. The method of claim 1, wherein the step of synchronizing the at least one backup node and the primary node further comprises the steps of:

transmitting synchronization information from the primary node to the at least one backup node.

5. The method of claim 4, wherein the step of transmitting synchronization information from the primary node to the at least one backup node further comprises the steps of:

transmitting at least one checkpoint message from the primary node to the at least one backup node, wherein

the at least one checkpoint message includes static information relating to the primary node as well as any outstanding session context for the primary node.

6. The method of claim 5, further comprising the steps of:

receiving, from the at least one backup node, a checkpoint message acknowledgment for each of said at least one checkpoint messages;

determining whether each of the checkpoint message acknowledgments were received prior to a change in flow state;

transmitting a synchronization declaration from the primary node to the at least one backup node if is it determined that each of the checkpoint message acknowledgments were received prior to a change in flow state; and

transmitting at least one new checkpoint message from the primary node to the backup node if is determined that each of the checkpoint packet acknowledgments was not received prior to a change in flow state.

7. The method of claim 4, further comprising the steps of:

periodically assessing synchronization maintenance between the primary node and the at least one backup node.

8. The method of claim 7, wherein the step of periodically assessing synchronization maintenance further comprises the step of:

transmitting at least a portion of internal state information from the primary node to the at least one backup node sufficient to permit replication of primary node traffic on the at least one backup node.

9. An apparatus for preventing information losses due to network node failure, the apparatus comprising:

a primary node;

at least one backup node operatively connected to the primary node;

synchronizing means operatively connected to the primary node and the backup node for synchronizing the at least one backup node and the primary node;

means for receiving ingress traffic in the primary node from a first endpoint;

means for replicating the ingress traffic to the at least one backup node;

means for outputting primary egress traffic from the primary node;

means for outputting backup egress traffic from the at least one backup node;

determining means operatively connected to the primary node and the at least one backup node for determining whether the primary node has failed;

means for transmitting the primary egress traffic from the primary node to a second endpoint if the determining means determine that the primary node has not failed; and

means for transmitting the backup egress traffic from a selected one of the at least one backup nodes to the second endpoint if the determining means determine that the primary node has failed.

10. The apparatus of claim 9, wherein the primary node and the at least one backup node are network routers.

11. The apparatus of claim 9, wherein the primary node and the at least one backup node are security engines for receiving encrypted ingress traffic and outputting decrypted egress traffic.

12. The apparatus of claim 9, wherein the synchronizing means further comprise:

means for transmitting synchronization information from the primary node to the at least one backup node.

13. The apparatus of claim 12, wherein the means for transmitting synchronization information further comprise:

means for transmitting at least one checkpoint message from the primary node to the at least one backup node, wherein the at least one checkpoint message includes static information relating to the primary node as well as any outstanding session context for the primary node.

14. The apparatus of claim 13, further comprising:

means for receiving in the primary node, from the at least one backup node, a checkpoint message acknowledgment for each of said at least one checkpoint packets;

second determining means for determining whether each of the checkpoint message acknowledgments were received prior to a change in flow state;

means for transmitting a synchronization declaration from the primary node to the at least one backup node if is it determined that each of the checkpoint message

acknowledgments were received prior to a change in flow state; and

means for transmitting at least one new checkpoint message from the primary node to the backup node if is determined that each of the checkpoint message acknowledgments was not received prior to a change in flow state.

15. The apparatus of claim 12, further comprising:

means for periodically assessing synchronization maintenance between the primary node and the at least one backup node.

16. The apparatus of claim 15, wherein the means for periodically assessing synchronization maintenance further comprise:

means for transmitting at least a portion of an internal state of the primary node to the backup node sufficient to permit replication of primary node traffic on the at least one backup node..

17. An article of manufacture for preventing information losses due to network node failure, the article of manufacture comprising:

at least one processor readable carrier; and

instructions carried on the at least one carrier;

wherein the instructions are configured to be readable from the at least one carrier by at least one processor and thereby cause the at least one processor to operate so as to:

synchronize a primary node and at least one operatively connected backup node;

receive, from a first endpoint, ingress traffic;

replicate the ingress traffic to the at least one backup node;

output, from the primary node, primary egress traffic related to the ingress traffic;

output, from the at least one backup node, backup egress traffic related to the ingress traffic;

determine if the primary node has failed;

transmit, from the primary node, primary egress traffic related to the ingress traffic to a second endpoint if it is determined that the primary node has not failed; and

transmit, from a selected one of the at least one backup nodes, backup egress traffic to the second endpoint if it is determined that the primary node has failed,

wherein the backup egress traffic replaces the primary egress traffic to the second endpoint and the selected one of the at least one backup nodes becomes the primary node for subsequent traffic.

18. The article of manufacture of claim 17, wherein the instructions further cause the at least one processor to operate so as to:

transmit synchronization information from the primary node to the at least one backup node.

19. The article of manufacture of claim 18, wherein the instructions further cause the at least one processor to operate so as to:

transmit at least one checkpoint message from the primary node to the at least one backup node, wherein the at least one checkpoint message includes static information relating to the primary node as well as any outstanding session context for the primary node.

20. The article of manufacture of claim 19, wherein the instructions further cause the at least one processor to operate so as to:

receive, from the at least one backup node, a checkpoint message acknowledgment for each of said at least one checkpoint messages;

determine whether each of the checkpoint message acknowledgments were received prior to a change in flow state;

transmit a synchronization declaration from the primary node to the at least one backup node if is it determined that each of the checkpoint message acknowledgments were received prior to a change in flow state; and

transmit at least one new checkpoint message from the primary node to the backup node if is determined that each of the checkpoint message acknowledgments was not received prior to a change in flow state.

21. The article of manufacture of claim 18, wherein the instructions further cause the at least one processor to operate so as to:

periodically assess synchronization maintenance between the primary node and the at least one backup node.

22. A computer data signal embodied in a carrier wave readable by a computing system and encoding a computer program of instructions for executing a computer process performing the method recited in claim 1.